PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-195735
(43)Date of publication of application : 30.07.1996

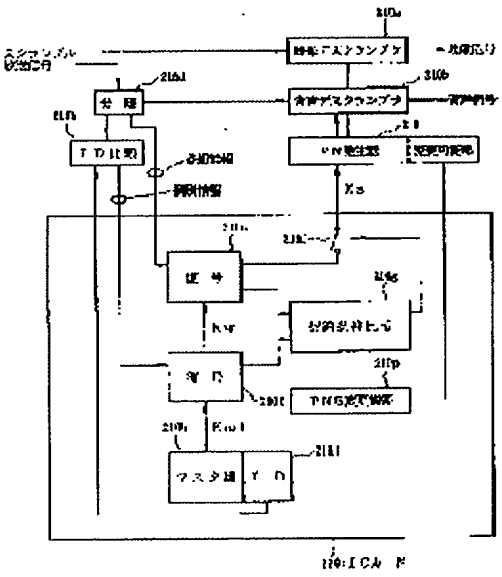
(51)Int.Cl. H04K 1/00
G09C 1/00
H04H 1/00
H04L 9/28

(21)Application number : 07-005792
(22)Date of filing : 18.01.1995

(71)Applicant : TOSHIBA CORP
(72)Inventor : OI SHINICHI

(54) DECODER

(57)Abstract:
PURPOSE: To keep secrecy by transiting a state sequentially from a state given by a scramble key and generating a PN signal based on a conversion logic from the state to be transited thereby making the logic changeable.
CONSTITUTION: Since a PN generator 310 revises a logic to generate a PN signal, the initial state of the generator 310 is transited sequentially based on PN information 210p when the PNG information 210p is available. A PN signal is given to a video descrambler 210a and an audio descrambler 210b based on the transition, from which descrambled video signal and audio signal are obtained. When PNG information 210p of an IC card 220 is given newly to the generator 310, the state transition is made different based on the new information 210p, a different PN signal is generated and descrambling is conducted based on the new PN signal. Since the logic for generating the PN signal is variable, the security is improved.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－195735

(43)公開日　平成８年(1996)７月30日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｋ　1/00				
Ｇ０９Ｃ　1/00		7259－5Ｊ		
Ｈ０４Ｈ　1/00	Ｆ			
	Ｈ			
			Ｈ０４Ｌ　9/02	Ａ

審査請求　未請求　請求項の数11　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平7－5792

(22)出願日　平成７年(1995)１月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　大井　伸一
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内

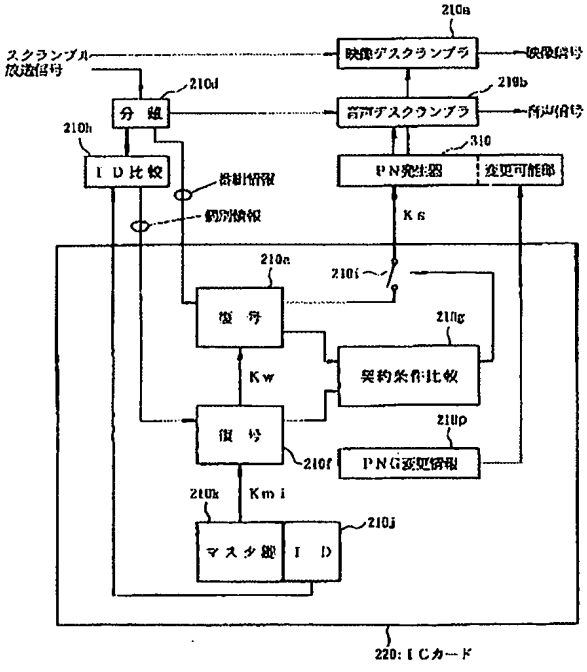
(74)代理人　弁理士　三好　秀和　（外３名）

(54)【発明の名称】　デコーダ装置

(57)【要約】

【目的】　ＩＣカードを使用したデコーダでもＰＮ発生器の安全性を向上することができるようにする。

【構成】　このデコーダは、スクランブルされた信号をＰＮ信号を用いてデスクランブルするであって、ＰＮ信号を用いて前記スクランブルされた信号をデスクランブルするデスクランブラ２１０ａ，２１０ｂと、ＰＮ信号生成ロジックに基づいてスクランブルキーによって与えられた状態から順次状態遷移しＰＮ信号を生成すると共に、ＰＮ信号生成ロジックが変更可能であるＰＮ発生器３１０と、スクランブルされた信号からスクランブルキーを復号すると共に、ＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえる制御部２２０と、を備える。



【特許請求の範囲】

【請求項１】　スクランブルされた信号をＰＮ信号を用いてデスクランブルするデコーダ装置であって、
前記ＰＮ信号を用いて前記スクランブルされた信号をデスクランブルするデスクランブラと、
スクランブルキーによって与えられた状態から順次状態遷移し、この遷移する状態から変換ロジックに基づいて前記ＰＮ信号を生成すると共に、前記ＰＮ信号生成のためのロジックが変更可能であるＰＮ発生器と、
前記スクランブルされた信号からスクランブルキーを復号すると共に、前記スクランブルキー及び前記ＰＮ信号生成ロジックを定めるための情報を前記ＰＮ発生器にあたえる制御部と、
を備えたデコーダ装置。

【請求項２】　前記ＰＮ発生器は、前記遷移する状態から前記ＰＮ信号を得るための信号を変換ロジックに基づいて生成すると共に、前記変換ロジックが変更可能である非線形ロジックを含んで構成されていることを特徴とする請求項１記載のデコーダ装置。

【請求項３】　前記ＰＮ発生器は、
前記スクランブルキーによって与えられた初期状態から順次状態遷移するとともに、その状態出力が変更可能であるレジスタ回路部と、
前記レジスタ回路部の状態出力を変換し前記ＰＮ信号を得るための信号を生成するロジック回路部と、
を含んで構成されていることを特徴とする請求項１記載のデコーダ装置。

【請求項４】　前記ＰＮ発生器は、前記スクランブルキーによって与えられた初期状態から順次状態遷移すると共に、その状態遷移のロジックが変更可能である線形フィードバックレジスタを含んで構成されていることを特徴とする請求項１記載のデコーダ装置。

【請求項５】　前記制御部は、ＩＤが書き込まれたＩＣカード上に構成され、前記スクランブルされた信号とともに送られたＩＤと前記ＩＣカード上のＩＤとが一致したときに前記スクランブルキーを前記ＰＮ発生器にあたえることを特徴とする請求項１記載のデコーダ装置。

【請求項６】　前記ＩＣカードの電源の状態を検出するための電源電圧検出回路をさらに有し、
前記制御部は、前記ＩＣカードが本体に挿入されたときに、前記ＰＮ信号生成のためのロジックを定めるための情報を前記ＰＮ発生器にあたえることを特徴とする請求項５記載のデコーダ装置。

【請求項７】　本体の電源の投入を検出するための電源電圧検出回路をさらに有し、
前記制御部は、本体の電源の投入が検出されたときに、前記ＰＮ信号生成ロジックを定めるための情報を前記ＰＮ発生器にあたえることを特徴とする請求項１記載のデコーダ装置。

【請求項８】　前記制御部は、前記ＰＮ信号生成ロジックの変更を示すＰＮＧ変更フラグが前記スクランブルされた信号とともに送られたときに前記ＰＮ信号生成ロジックを定めるための情報を前記ＰＮ発生器にあたえることを特徴とする請求項１記載のデコーダ装置。

【請求項９】　前記制御部は、前記ＰＮ信号生成ロジックを定めるための情報を複数有し、前記ＰＮ信号生成ロジックを定めるための情報を選択するためのＰＮＧ選択情報と前記ＰＮ信号生成ロジックの変更を示す前記ＰＮＧ変更フラグとが前記スクランブルされた信号とともに送られたときに、前記ＰＮＧ選択情報に応じた前記ＰＮ信号生成ロジックを定めるための情報を選択して前記ＰＮ発生器にあたえることを特徴とする請求項１記載のデコーダ装置。

【請求項１０】　本体側にデコーダのＩＤを記憶するためのＩＤメモリと、
前記ＩＤメモリに記憶されたＩＤと前記ＩＣカード上のＩＤとが一致したときにのみ前記スクランブルキーを前記ＰＮ発生器にあたえる比較器をさらに有することを特徴とする請求項１記載のデコーダ装置。

【請求項１１】　前記制御部は、前記ＩＤメモリにＩＤが記憶されていない場合に、前記ＩＣカード上のＩＤを書き込むことを特徴とする請求項１０記載のデコーダ装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、映像及び音声信号をスクランブルして放送し、デコーダでデスクランブルして視聴する有料放送システムにおいて、受信側でデスクランブルして視聴するためのデコーダ装置に関する。

【０００２】

【従来の技術】衛星を利用した放送では、映像及び音声信号をスクランブルして放送し、デコーダでデスクランブルして視聴する有料放送がある。この有料放送のシステムの一例が昭和６３年１１月に電気通信技術審議会により答申された「衛星放送によるテレビジョン放送における有料方式に関する技術的条件」に対する答申（文献１）に示されている。図９は、文献１に示された有料放送のシステム構成を示したものであり、そのスクランブル方式としてＰＮ信号（pcuzo random noize：疑似ランダムノイズ信号）加算式が用いられている。

【０００３】この有料放送のシステムでは、放送局１１０からデコーダ２１０に送られる放送信号には、スクランブルされた映像信号とサブ信号とが含まれ、サブ信号には、スクランブルされたデジタル音声信号及び番組情報，デコーダ２１０についての個別情報が含まれる。

【０００４】放送局１１０側では、デコーダ２１０についての個別情報であるワーク鍵Ｋｗ，契約内容，デコーダＩＤのうちデコーダＩＤを用いてマスタ鍵ファイル１１０ｇからマスタ鍵Ｋｍｉを得て、マスタ鍵Ｋｍｉを用いて個別情報の暗号化が行われる（１１０ｆ）。また、ワー

ク鍵Ｋｗを用いて、スクランブル鍵Ｋｓ，放送局識別．サービス．年月などの番組情報の暗号化が行われる（１１０ｅ）。

【０００５】本件には直接関係がないためスクランブル方式の詳細は示さないが、音声信号、映像信号は、映像スクランブラ１１０ａ．音声スクランブラ１１０ｂでＰＮ信号を使用してスクランブルされる。スクランブルのためのＰＮ信号は、ＰＮ信号発生器１１０ｃから与えられ、その信号は順次変化するランダムデータである。ＰＮ信号発生器１１０ｃの初期状態はスクランブル鍵Ｋｓによって与えられる。スクランブルされた音声信号は、ＰＮ信号発生器を初期化するタイミング、暗号化された番組情報及び個別情報とともに多重化されてサブ信号（副信号）となる（１１０ｄ）。このサブ信号とスクランブルされた映像信号とが放送信号として放送電波として放送局１１０から出力される。

【０００６】放送信号は、ワーク鍵Ｋｗ、マスタ鍵Ｋmiを用いた３重の暗号化構造によって秘話性を高めている。また、個別情報は、電話回線やＩＣカードを介して該当するデコーダ２１０に送ることもできる。

【０００７】デコーダ２１０では、放送信号のサブ信号から音声信号、番組情報、個別情報を分離する（２１０ａ）。分離された個別情報はそのデコーダのマスタ鍵Ｋmiを用いて復号され保存される（２１０ｆ）。この復号２１０ｆは暗号化１１０ｆと同じマスタ鍵Ｋmiでなければ正しく行えようになっているので、当該マスタ鍵Ｋmiを持つデコーダのみが個別情報を復号できる。番組情報は、復号して得た個別情報のうちのワーク鍵Ｋｗを用いて復号されるが（２１０ｅ）、この場合も、暗号化１１０ｅと同じワーク鍵Ｋｗでなければ正しく番組情報が復号できないようになっている。こうして復号して得た番組情報、個別情報は、契約条件比較回路２１０ｇで比較されて、契約条件が合いデスクランブルしても良いと判定された場合にのみ、ＰＮ発生器２１０ｃを動作させ、番組情報中のスクランブル鍵Ｋｓを用いてＰＮ信号を発生させる。映像デスクランブラ２１０ａ．音声デスクランブラ２１０ｂでは、このＰＮ信号を用いて加算などによりデスクランブルが行われる。

【０００８】スクランブル鍵Ｋｓは、音声信号、映像信号をデスクランブルするのに必要な値であり、スクランブルの場合と同じ値の場合にのみ、音声信号、映像信号のデスクランブルが行われて出力される。スクランブル鍵Ｋｓを復元するにはワーク鍵Ｋｗを要するので、ワーク鍵Ｋｗを持たないデコーダは正しいスクランブル鍵Ｋｓが得られないようになっている。さらに、ワーク鍵Ｋｗを変更可能なようにワーク鍵Ｋｗを含む個別情報を放送局１１０から送出し、契約継続を望む視聴者のデコーダにのみ個別情報を与えるようになっている。そして、ワーク鍵Ｋｗを含む個別情報を復元するにはマスタ鍵Ｋmiを要し、当該マスタ鍵Kmiを持つデコーダのみが個別情報を受け取れるようになっている。マスタ鍵Kmiは、個々のデコーダごとに異なるような値に設定されている。その値は、デコーダが視聴者の手に渡る前に、例えば工場出荷時に予め設定されている。

【０００９】上述のような有料放送のデコーダでは、デコーダ内の暗号復号処理や契約条件の比較といった処理はマイコンシステムを用いて行うのが一般的である。そして、このマイコンシステムを含む回路をＩＣカードにして交換可能にすることも行われている。図１０は、暗号復号処理や契約条件の比較をこのＩＣカードで行うようにしたデコーダの構成例を示したものである。

【００１０】この図１０のデコーダは、図９のデコーダ２１０とほぼ同じ構成を有し、上記処理を行うためのマイコンシステムはＩＣカード２２０に搭載されている。ＩＣカード２２０とデコーダ本体とはコネクタを介して信号をやり取りできるようになっている。そして、ＩＣカード２２０はマスタ鍵Kmiのほかにｒｏｍなどの不揮発メモリに書き込まれたＩＤ２１０ｊを有し、デコーダ本体にはＩＤ比較器２１０ｈが設けられている。放送信号のサブ信号から分離した個別情報に含まれるＩＤとＩＣカード２２０のＩＤ２１０ｊとをＩＤ比較器２１０ｈで比較して、一致した場合にＩＣカード２２０に個別情報を与えるようにしている。番組情報、個別情報を復号し契約条件があっていた場合にスイッチ２１０ｉをＯＮにしてスクランブル鍵ＫｓをＰＮ発生器２１０ｃに与えるようになっている。こうして、個別情報の選別を行い、ＩＣカード２２０に与えられている個別情報からその契約者のみに視聴を制限するようにしている。なお、ＩＤ比較器２１０ｈは、ＩＣカードとの通信データ速度に制限があるために、必要な回路である。

【００１１】図１１は、上記文献１に示されているＰＮ発生器２１０ｃの構成例を示したものである。このＰＮ発生器は、線形フィードバックシフトレジスタ（ＬＦＳＲ）２１１ａ．２１１ｂ．２１１ｃと非線形ロジック（ＮＦ）２１２ａ．２１２ｂ．２１２ｃとの組み合わせ回路例である。

【００１２】スクランブル鍵Ｋｓは、放送信号のサブ信号から得たロードタイミングパルスがあるときにＬＦＳＲ２１１ａ～２１１ｃに取り込まれ、ＰＮ信号発生器の初期化が行われる。スクランブル鍵Ｋｓのうち１３ビットはＬＦＳＲ２１１ａの各レジスタに、１１ビットはＬＦＳＲ２１１ｂの各レジスタに、８ビットはＬＦＳＲ２１１ｃの各レジスタに与えられる。

【００１３】ＬＦＳＲ２１１ａ～２１１ｃには、音声信号、映像信号に同期したシフトクロックがあたえられており、ＬＦＳＲ２１１ａ～２１１ｃのレジスタのうちそれぞれ６つのレジスタからの出力がＮＦ２１２ａ～２１２ｃに与えられる。ＮＦ２１２ａ～２１２ｃは、ＲＯＭを用いて構成され、ＬＦＳＲ２１１ａ～２１１ｃからの６ビット出力をそのマスクパターンに従った一定の非線

形ロジックで変換し、１ビットで出力する。切替えスイッチ２１４は、ＮＦ２１２ｂからの切り替え信号に応じて、ＮＦ２１２ａ，２１２ｃを切り替えて排他的論理和回路（ＥＸ－ＯＲ）２１３に与える。ＥＸ－ＯＲ２１３にはＬＦＳＲ２１１ａの１つのレジスタの出力が与えられており、これとＮＦ２１２ａまたはＮＦ２１２ｃの出力のＥＸ－ＯＲがＰＮ信号として映像デスクランブラ２１０ａ，音声デスクランブラ２１０ｂに出力される。

【００１４】ＬＦＳＲ２１１ａ～２１１ｃの状態は、スクランブル鍵Ｋｓが与えられた時の初期状態からシフトクロックに応じて遷移し、それにともなってＮＦ２１２ａ～２１２ｃの出力も変化する。このようにランダムに変化する状態から得たランダムなＰＮ信号をもちいてデスクランブルが行われる。

【００１５】なお、この例では、ＮＦ２１２ａ～２１２ｃを用いているが、ＬＦＳＲ２１１ａ～２１１ｃの各１ビット分のレジスタ出力を直接切替えスイッチ２１４やＥＸ－ＯＲ２１３に与えたり、ＰＮ信号として用いる構成もある。

【００１６】

【発明が解決しようとする課題】上述のようなデコーダでは、マスタ鍵Kmi、復号アルゴリズム、ＰＮ発生器の内容が第３者に知られてしまうとシステムの安全性の低下を招くことになる。そのため、例えば図９の例では、デコーダ２１０に使用する映像デスクランブラ２１０ａ，音声デスクランブラ２１０ｂ，ＰＮ発生器２１０ｃおよびマイコンシステムを１チップのＩＣにするなどによって対策することが必要である。

【００１７】また、図１０のようにＩＣカード２２０を利用したデコーダでは、ＩＣカード２２０からＰＮ発生器２１０ｃにスクランブル鍵Ｋｓを与えることになるため、スクランブル鍵ＫｓとＰＮ信号の関係からＰＮ発生器２１０ｃの構成を第３者に知られてしまう可能性があるという問題があった。

【００１８】そこで、本発明はＩＣカードを使用したデコーダでもＰＮ発生器の安全性を向上することができるようにすることをその目的とする。

【００１９】

【課題を解決するための手段】上記目的を達成するために、本願請求項１に係る発明は、スクランブルされた信号をＰＮ信号を用いてデスクランブルするデコーダ装置であって、ＰＮ信号を用いて前記スクランブルされた信号をデスクランブルするデスクランブラと、スクランブルキーによって与えられた状態から順次状態遷移し、この遷移する状態から変換ロジックに基づいてＰＮ信号を生成すると共に、ＰＮ信号生成のためのロジックが変更可能であるＰＮ発生器と、スクランブルされた信号からスクランブルキーを復号すると共に、前記スクランブルキー及びＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえる制御部と、を備える。

【００２０】本願請求項２に係る発明は、上記請求項１の構成に加えて、前記遷移する状態から前記ＰＮ信号を得るための信号を変換ロジックに基づいて生成すると共に、前記変換ロジックが変更可能である、非線形ロジックと、を含んで構成されていることを特徴とする。

【００２１】本願請求項３に係る発明は、上記請求項１の構成に加えて、ＰＮ発生器は、スクランブルキーによって与えられた初期状態から順次状態遷移するとともに、その状態出力が変更可能であるレジスタ回路部と、レジスタ回路部の状態出力を変換しＰＮ信号を得るための信号を生成するロジック回路部とを含んで構成されていることを特徴とする。

【００２２】本願請求項４に係る発明は、上記請求項１の構成に加えて、ＰＮ発生器は、スクランブルキーによって与えられた初期状態から順次状態遷移すると共に、その状態遷移のロジックが変更可能である線形フィードバックレジスタを含んで構成されていることを特徴とする。

【００２３】本願請求項５に係る発明は、上記請求項１の構成に加えて、制御部は、ＩＤが書き込まれたＩＣカード上に構成され、スクランブルされた信号とともに送られたＩＤとＩＣカード上のＩＤとが一致したときにスクランブルキーをＰＮ発生器にあたえることを特徴とする。

【００２４】本願請求項６に係る発明は、上記請求項５の構成に加えて、ＩＣカードの電源の状態を検出するための電源電圧検出回路をさらに有し、制御部は、ＩＣカードが本体に挿入されたときに、ＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえることを特徴とする。

【００２５】本願請求項７に係る発明は、上記請求項１の構成に加えて、本体の電源の投入を検出するための電源電圧検出回路をさらに有し、制御部は、本体の電源の投入が検出されたときに、ＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえることを特徴とする。

【００２６】本願請求項８に係る発明は、上記請求項１の構成に加えて、制御部は、ＰＮ信号生成ロジックの変更を示すＰＮＧ変更フラグがスクランブルされた信号とともに送られたときにＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえることを特徴とする。

【００２７】本願請求項９に係る発明は、上記請求項１の構成に加えて、制御部は、ＰＮ信号生成ロジックを定めるための情報を複数有し、ＰＮ信号生成ロジックを定めるための情報を選択するためのＰＮＧ選択情報とＰＮ信号生成ロジックの変更を示すＰＮＧ変更フラグとがスクランブルされた信号とともに送られたときに、ＰＮＧ選択情報に応じたＰＮ信号生成ロジックを定めるための情報を選択してＰＮ発生器にあたえることを特徴とする。

【００２８】本願請求項１０に係る発明は、上記請求項１の構成に加えて、本体側にデコーダのＩＤを記憶するためのＩＤメモリと、ＩＤメモリに記憶されたＩＤとＩＣカード上のＩＤとが一致したときにのみスクランブルキーをＰＮ発生器にあたえる比較器をさらに有することを特徴とする。

【００２９】本願請求項１１に係る発明は、上記請求項１０の構成に加えて、制御部は、ＩＤメモリにＩＤが記憶されていない場合に、ＩＣカード上のＩＤを書き込むことを特徴とする。

【００３０】

【作用】本願請求項１に係る発明によれば、制御部からの情報に応じて、ＰＮ発生器のＰＮ信号生成のためのロジックを変更することが可能であり、この変更によって生成するＰＮ信号も異なってくる。すなわち実質的にＰＮ発生器の構成が異なったものとして動作し、これによって得たＰＮ信号でデスクランブルが行われるので、ＰＮ発生器のＰＮ信号生成のためのロジック構成を解明するために、新手名手間が必要になる。したがって、そのロジック構成を容易に知り得ないため、機密性を保持することができ、デコーダのセキュリティを高いものにすることができる。

【００３１】本願請求項２，３又は４に係る発明によれば、ＰＮ発生器が、上記の順次状態遷移するレジスタおよび非線形ロジック又はロジック回路部で構成され、非線形ロジックの変換ロジックが変更可能であること、または、線形フィードバックレジスタの状態遷移のロジックが変更可能であることにより、ＰＮ信号生成のためのロジックを変更することが可能であり、本願請求項１と同様に、よりその内部構成を外部から分かりにくくなる。

【００３２】本願請求項５に係る発明によれば、ＩＤとが一致したときにスクランブルキーがＰＮ発生器にあたえられることにより、個別の条件に応じてデスクランブルを行いうる。

【００３３】本願請求項６に係る発明によれば、ＩＣカードが本体に挿入されたときに、ＰＮ信号生成ロジックを定めるための情報がＰＮ発生器にあたられることにより、電源オフ時にその内容が消えてしまってもよいような回路でもよいので、ハードウェアのコストが安いものにし得る。。

【００３４】本願請求項７に係る発明によれば、起動時にＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえるので、電源オフ時にＰＮ信号生成ロジックを定めるための情報を保持しなくてもよい構成にし得る。

【００３５】本願請求項８に係る発明によれば、ＰＮ信号生成ロジックの変更を示すＰＮＧ変更フラグがスクランブルされた信号とともに送られたときにＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえるので、ＰＮ発生器の動作は番組に応じて変えることができるため、番組についても機密性を保持することができ、番組のセキュリティも高いものになる。

【００３６】本願請求項９に係る発明によれば、ＰＮＧ選択情報とＰＮＧ変更フラグとが送られたときに、ＰＮＧ選択情報に応じたＰＮ信号生成ロジックを定めるための情報を選択してＰＮ発生器にあたえるので、ＰＮ信号生成ロジックの選択の幅が広くなると共にＰＮ発生器の動作は番組に応じて変えることができるため、番組についてもより機密性を保持することができ、番組のセキュリティもより高いものになる。

【００３７】本願請求項１０に係る発明によれば、ＩＤメモリに記憶されたＩＤとＩＣカード上のＩＤとが一致したときにのみスクランブルキーをＰＮ発生器にあたえることにより、機器のセキュリティをより高めることができる。

【００３８】本願請求項１１に係る発明によれば、ＩＤメモリに記憶されたＩＤとＩＣカード上のＩＤとが一致したときにのみスクランブルキーがＰＮ発生器にあたえられ、ＩＤが一致したときにのみデコーダ本体の使用が可能になるので、デコーダ本体のセキュリティがより高いものになる。

【００３９】

【実施例】本発明の実施例を図面を参照して説明する。なお、前述の従来例と同一もしくは同等の構成要素については同一の符号を用いると共に、その説明を簡略化しもしくは省略するものとする。

【００４０】図１は、第１の実施例にかかるデコーダの構成を示したものである。このデコーダは、前述の従来例と同様に、スクランブルされた放送信号のサブ信号から音声信号、番組情報、個別情報を分離する回路２１０ｄと、放送信号のスクランブルされた映像信号をデスクランブルし映像信号にする映像デスクランブラ２１０ａ、サブ信号から得たスクランブルされた音声信号をデスクランブルし音声信号にする音声デスクランブラ２１０ｂと、個別情報に含まれるＩＤとＩＣカード２２０のＩＤ２１０ｊとを比較するためのＩＤ比較器２１０ｈとを有する。また、このデコーダは、各種処理を行う点に付いても前述の従来例と同様であるが、マイコンシステムの一部の処理と、ＰＮ発生器３１０の構成が異なっており、この点に特徴がある。

【００４１】ＰＮ発生器３１０は、スクランブルキーによって与えられた初期状態から順次状態遷移しこの遷移する状態から変換ロジックに基づいてＰＮ信号を生成するための回路であるが、そのＰＮ信号生成のためのロジックに変更可能部があり、すなわちＰＮ信号生成のためのロジックが変更可能な点に特徴がある。図２および３は、このＰＮ発生器３１０の構成例を示したものである。

【００４２】図２のＰＮ発生器３１０は、その内容が変

更可能な非線形ロジック（ＮＦ）３１２ａ，３１２ｂ，３１２ｃを用いて構成したものである。

【００４３】ＬＦＳＲ２１１ａ～２１１ｃは、ロードタイミングパルスがあるときにスクランブル鍵Ｋｓの１３ビット、１１ビット、８ビットをそれぞれ取り込み、シフトクロックに応じてＬＦＳＲ２１１ａ～２１１ｃの状態は、スクランブル鍵Ｋｓが与えられた時の初期状態から遷移する。

【００４４】ＮＦ３１２ａ，３１２ｂ，３１２ｃは、ＥＰＲＯＭまたはＲＡＭなど電気的にその内容が変更可能な回路を用いて構成され、ＩＣカード２２０のマイコンシステムからのＰＮＧ情報２１０ｐが書き込めるようになっている。そして、書き込まれたＰＮＧ情報２１０ｐに従った非線形ロジックで変換し、ＰＮ信号生成のための信号を１ビットで出力する。切替えスイッチ２１４は、ＮＦ２１２ｂからの切り替え信号に応じて、ＮＦ２１２ａ，２１２ｃを切り替えてＥＸ－ＯＲ２１３に与える。ＥＸ－ＯＲ２１３にはＬＦＳＲ２１１ａの１つのレジスタの出力が与えられており、これとＮＦ２１２ａまたはＮＦ２１２ｃの出力のＥＸ－ＯＲがＰＮ信号として映像デスクランブラ２１０ａ，音声デスクランブラ２１０ｂに出力される。

【００４５】ＬＦＳＲ２１１ａ～２１１ｃの状態は、スクランブル鍵Ｋｓが与えられた時の初期状態からシフトクロックに応じて遷移し、それにともなってＮＦ２１２ａ～２１２ｃの出力も変化する。こうした状態遷移にともなってランダムなＰＮ信号を生成する点に付いては前述の従来例と同様であるが、図２のＰＮ発生器３１０では、生成されたＰＮ信号は、ＮＦ２１２ａ～２１２ｃに書き込まれたＰＮＧ情報２１０ｐに応じて異なったものになる。

【００４６】この様に、図２のＰＮ発生器３１０は、非線形ロジック３１２ａ，３１２ｂ，３１２ｃの変換ロジックを変更するようにして、ＰＮ信号生成のためのロジックを変更可能にしている。

【００４７】図３のＰＮ発生器３１０は、ＬＦＳＲ２１１ａ～２１１ｃの状態出力を可変にすることにより、等価的に変換ロジックを変更可能にしたものである。

【００４８】この図３のＰＮ発生器３１０は、従来例と同様のＬＦＳＲ２１１ａ～２１１ｃ、ＮＦ２１２ａ～２１２ｃ、切替えスイッチ２１４、ＥＸ－ＯＲ２１３を用いている。そして、ＬＦＳＲ２１１ａ～２１１ｃとＮＦ２１２ａ～２１２ｃとの間に、マルチプレクサ３１５ａ～３１５ｃを接続しＬＦＳＲ２１１ａ～２１１ｃとともにレジスタ回路部を構成している。マルチプレクサ３１５ａはＬＦＳＲ２１１ａの１３のレジスタ出力から６つを、マルチプレクサ３１５ｂはＬＦＳＲ２１１ｂの１１のレジスタ出力から６つをマルチプレクサ３１５ｃはＬＦＳＲ２１１ｃの８のレジスタ出力から６つをＩＣカード２２０のマイコンシステムからのＰＮＧ情報２１０ｐに基づく信号に応じて選択してＮＦ２１２ａ～２１２ｃに与える。そして、ＮＦ２１２ａ～２１２ｃはレジスタ回路部の出力を変換してＰＮ信号生成のための信号を得るためのロジック回路である。

【００４９】こうしてＬＦＳＲ２１１ａ～２１１ｃのレジスタ出力を切り替えてＮＦ２１２ａ～２１２ｃに与えることで、ＰＮ信号生成のためのロジックが変更可能になっている。

【００５０】ＬＦＳＲ２１１ａ～２１１ｃの一般的構成としては、図１２（ａ）のように、Ｍ系列のＰＮ符号を発生するものが知られている。このＬＦＳＲは、ｎ段のシフトレジスタ２１１１とＥＸＯＲ２１１２で構成され、シフトレジスタ２１１１のｋ段（$1 \leqq k \leqq n$）目の状態を順次ＥＸＯＲ演算してシフトレジスタ２１１１の初段の入力として与え、シフトレジスタ２１１１にシフトクロックを与えることにより状態遷移していくようになっている。

【００５１】ＬＦＳＲ２１１ａ～２１１ｃとして、本件発明者が考案した図１２（ｂ）のような回路も用い得る。この回路は、シフトレジスタ２１１１の所定の出力を順次ＥＸＯＲ演算する第１のＥＸＯＲ２１１２ａと、これとは異なるシフトレジスタ２１１１の出力を順次ＥＸＯＲ演算する第２のＥＸＯＲ２１１２ｂと（さらに、第３，第４のＥＸＯＲを設けるようにしても良い）、これらの演算結果をＰＮＧ情報２１０ｐに応じて切り替えるセレクタ２１１３とを有している点が、図１２（ｂ）の回路とは異なっている。この構成により、ＰＮＧ情報２１０ｐに応じてＬＦＳＲの状態遷移のロジックが変更されることにより、ＰＮ信号生成のためのロジックが変更可能になっている。

【００５２】図１のＩＣカード２２０には、制御部であるマイコンシステムが搭載されており、図ではその処理ブロックを示している。ＩＣカード２２０にはマスタ鍵Ｋｍｉ及びＩＤ２１０ｊが書き込まれ、ＩＣカード２２０は、従来例と同様に、分離された個別情報からマスタ鍵Ｋｍｉを用いて復号され保存する処理ブロック２１０ｆ、復号して得た個別情報のうちのワーク鍵Ｋｗを用いて番組情報を復号する処理ブロック２１０ｅ、番組情報及び個別情報から契約条件を比較し契約条件が合致しているかを判断する処理ブロック２１０ｇ、番組情報のうちスクランブル鍵ＫｓをＰＮ発生器２１０ｃに与える処理ブロック２１０ｉを有する。これらにより、従来例と同様に、マスタ鍵Ｋｍｉ及びＩＤ２１０ｊが合致し、かつ、契約条件が合いデスクランブルしても良いと判定された場合に、処理ブロック２１０ｉでスクランブル鍵Ｋｓを与えてＰＮ発生器２１０ｃを動作させ、視聴できるようになっている。さらに、ＩＣカード２２０は、ＰＮ発生器３１０の変換ロジックを定めるためのＰＮＧ情報がそのＲＯＭに書き込まれ、ＩＣカード２２０のマイコンシステムは、ＰＮＧ情報２１０ｐをＰＮ発生器３１０に与え

るようになっている。

【００５３】図１のデコーダの動作は、ＰＮ発生器３１０およびＰＮＧ情報２１０ｐに関係するところを除いて従来例と同じである。回路２１０ｄでサブ信号から音声信号、番組情報、個別情報が分離され、個別情報に含まれるＩＤとＩＣカード２２０のＩＤ２１０ｊとがＩＤ比較器２１０ｈで比較され、一致した場合に、ＩＣカード２２０の処理ブロック２１０ｆでマスタ鍵Ｋｍｉを用いて個別情報が復号される。また、処理ブロック２１０ｅで個別情報のうちのワーク鍵Ｋｗを用いて番組情報が復号され、処理ブロック２１０ｇで契約条件が合致していると判断されたときに、番組情報に含まれるスクランブル鍵ＫｓがＰＮ発生器３１０に与えられる。

【００５４】ここで、ＰＮ発生器３１０はそのＰＮ信号生成のためのロジックが変更可能であることから、すでにＰＮＧ情報２１０ｐがあれば、ＰＮ発生器３１０は、そのＰＮＧ情報２１０ｐに基づいて初期状態から順次状態が遷移し、それに応じたＰＮ信号を映像デスクランブラ２１０ａ、音声デスクランブラ２１０ｂに与え、デスクランブルされた映像信号、音声信号が得られる。ＰＮ発生器３１０は、ＩＣカード２２０のＰＮＧ情報２１０ｐが新たに与えられると、新たなＰＮＧ情報２１０ｐに基づいてその状態遷移が異なったものになり、異なったＰＮ信号を生成し、実質的にその構成が異なったものとして動作する。こうして得た新たなＰＮ信号でデスクランブルが行われるようになる。

【００５５】この様に、このデコーダでは、ＰＮ発生器３１０がＰＮ信号生成のためのロジックが変更可能であることから、ＰＮ信号生成のためのロジックが一定ではなく可変になっているので、その構成を容易に知り得ない。そのため、機密性を保持することができ、このデコーダは、セキュリティが高いものになる。

【００５６】次に、第２の実施例について説明する。

【００５７】この第２の実施例にかかるデコーダの構成は、図４に示すように、前述の第１の実施例と同様の構成を有するのであるが、ＩＣカード２２０に電源電圧を監視する電源監視回路３３０が設けられている点が第１の実施例と異なっている。そして、電源監視回路３３０が電源がオンになるのを検知したときに、ＩＣカード２２０のマイコンシステムはＰＮＧ情報２１０ｐをＰＮ発生器３１０に与えるようになっている。

【００５８】この第２の実施例にかかるデコーダでは、ＩＣカード２２０が挿入された状態でデコーダの電源をオンにすると、電源監視回路３３０によって電源オンが検知される。ＩＣカード２２０のＰＮＧ情報２１０ｐがＰＮ発生器３１０に与えられ、ＰＮ発生器３１０はＰＮ信号の生成ができるようになる。ＩＣカード２２０が挿入された後の動作は第１の実施例と同じであり、ＰＮ発生器３１０がＰＮ信号生成のためのロジックが変更可能であることから、機密性を保持することができ、このデコーダは、セキュリティが高いものになる。

【００５９】この実施例の場合、起動時に、ＩＣカード２２０からのＰＮＧ情報２１０ｐを与えるようにしていることから、ＰＮ発生器３１０は、電源オフ時にＰＮＧ情報２１０ｐを保持しておく必要はなくなる。したがって、図２のようなＰＮ発生器３１０を用いた場合、電源オフ時にその内容が消えてしまってもよいような回路、例えばＲＡＭでもよいので、ハードウェアのコストが安くなるという利点がある。

【００６０】次に、第３の実施例について説明する。

【００６１】この第３の実施例にかかるデコーダの構成は、前述の第２の実施例と同様の図４の構成を有するのであるが、ＩＣカード２２０が挿入されたときにＩＣカード２２０のマイコンシステムがＰＮＧ情報２１０ｐをＰＮ発生器３１０に与えるようになっている点が異なっている。電源監視回路３３０はＩＣカード２２０内部の電源の状態を監視し、ＩＣカード２２０の挿入によって電源がオンになるのを検知したときにマイコンシステムに信号を与えるようになっており、この信号によってマイコンシステムはデコーダ本体と最初の通信の際にＰＮＧ情報２１０ｐをＰＮ発生器３１０に与える。

【００６２】この第３の実施例にかかるデコーダでは、ＩＣカード２２０の挿入によってＰＮＧ情報２１０ｐがＰＮ発生器３１０に与えられ、ＰＮ発生器３１０はＰＮ信号の生成ができるようになる。ＩＣカード２２０が挿入された後の動作は第１の実施例と同じであり、ＰＮ発生器３１０がＰＮ信号生成のためのロジックが変更可能であることから、機密性を保持することができ、このデコーダは、セキュリティが高いものになる。この実施例の場合、電源オフ時にその内容が消えない回路、例えばＥＥＰＲＯＭを用いることを要するが、その反面ＰＮＧ情報２１０ｐがＰＮ発生器３１０に保持されていることから、ＰＮＧ情報２１０ｐを持っているＩＣカード２２０だけでなくＰＮＧ情報２１０ｐを持っていないものも用いることができる。

【００６３】次に、第４の実施例について説明する。

【００６４】この第４の実施例にかかるデコーダの構成は、図５に示すように、前述の第１の実施例と同様の構成を有するのであるが、番組情報に含まれるＰＮＧ変更フラグに応じてマイコンシステムがＰＮＧ情報２１０ｐをＰＮ発生器３１０に与えるようになっている点が第１の実施例と異なっている。

【００６５】放送局側からは、ＰＮＧ変更フラグを含む番組情報を送り、デコーダ側でＰＮＧ変更フラグを検出した場合、マイコンシステムはＰＮＧ情報２１０ｐをＰＮ発生器３１０に与えてＰＮ発生器３１０の動作を変更する。放送局側から番組に応じてＰＮＧ変更フラグを送ることにより、ＰＮ発生器３１０の動作は番組に応じて変化するようになる。そのため、番組についても機密性を保持することができ、このデコーダだけでなく番組の

セキュリティが高いものになる。

【００６６】次に、第５の実施例について説明する。

【００６７】この第５の実施例にかかるデコーダの構成は、図６に示すように、前述の第４の実施例と同様の構成を有するのであるが、複数のＰＮＧ情報２１０p1，２１０p2 を有し、番組情報に含まれるＰＮＧ変更フラグに応じてマイコンシステムがＰＮＧ情報２１０ｐをＰＮ発生器３１０に与えるうえに、番組情報に含まれるＰＮＧ選択情報に応じてＰＮ発生器３１０に与えるＰＮＧ情報をマイコンシステムが選択するような処理ブロック２１０ｍを有する点が第１の実施例と異なっている。

【００６８】放送局側からは、ＰＮＧ変更フラグ及びＰＮＧ選択情報を含む番組情報を送り、デコーダ側でＰＮＧ変更フラグを検出した場合、マイコンシステムはＰＮＧ選択情報に応じたＰＮＧ情報２１０p1，２１０p2 を選択してＰＮ発生器３１０に与える。ＰＮ発生器３１０は、ＰＮＧ選択情報に応じた動作に変更される。このように、放送局側から番組に応じてＰＮＧ変更フラグ及びＰＮＧ選択情報を送ることにより、ＰＮ発生器３１０の動作は番組に応じて変化するようになる。そのため、番組についてより機密性を保持することができ、このデコーダだけでなく番組のセキュリティがより高いものになる。

【００６９】次に、第６の実施例について説明する。

【００７０】この第６の実施例にかかるデコーダの構成は、図７に示すように、前述の第１の実施例と同様の構成を有するのであるが、デコーダの側にデコーダのＩＤを記憶しておくためのＩＤメモリ３３０と、ＩＤメモリ３３０に記憶されたＩＤとＩＣカード２２０内のＩＤ２１０ｊとを比較する比較器４１０ｈとを有する点が第１の実施例と異なっている。そして、比較器４１０ｈは、ＩＤメモリ３３０に記憶されたＩＤとＩＣカード２２０内のＩＤ２１０ｊとが一致したときに、ＩＣカード２２０からのＰＮＧ情報２１０をＰＮ発生器３１０に与えるようになっている。

【００７１】図８は、このデコーダのＰＮＧ変更の処理フローを示したもので、本実施例では、ＩＣカード２２０のマイコンシステムは、上記第１の実施例の処理に加えて、ＩＤメモリ３４０に関する処理を行う。

【００７２】ＩＣカード２２０のマイコンシステムは、ＩＤメモリ３４０からよみだしてＩＤメモリ３４０にＩＤが記憶されているかを判定し、ＩＤが記憶されていなかった場合（例えば、すべてのビットが０の場合）、ＩＣカード２２０のＩＤ２０１ｊの値をＩＤメモリ３４０に書き込む、という処理を行う（図８の符号８１０、８２０）。これによって、ＩＤメモリ３４０にＩＤが記憶されていない初期状態において場合、最初に差し込まれたＩＣカード２２０のＩＤがデコーダ本体のＩＤメモリ３４０に書き込まれる。

【００７３】電源オン後、最初に差し込まれたＩＣカード２２０のＩＤがＩＤメモリ３４０に記憶され、以降このＩＤとＩＣカード２２０のＩＤとが比較器４１０ｈによって比較される。そして、これらが一致したときのみ、ＩＣカード２２０からのＰＮＧ情報２１０によりＰＮ発生器３１０の動作を変更できるようになる。そして、前述の実施例に示したＰＮＧ変更情報の要求があると、ＰＮＧ情報２１０がＰＮ発生器３１０に与えられる。

【００７４】なお、この実施例の場合でも、ＩＣカード２２０にＰＮＧ情報が無い場合は、ＰＮ発生器３１０の動作を変更でき無い。

【００７５】この様に、この実施例では、ＩＤメモリ３４０に記憶されたＩＤとＩＣカード２２０内のＩＤ２１０ｊとを比較することによって、一致するＩＣカード２２０の場合だけ、ＰＮ発生器３１０の動作を変更できるようになるので、機器のセキュリティをより高めることができる。

【００７６】本発明は、上述の実施例に限られず、様々な変形が可能である。

【００７７】例えば、第２の実施例でＩＣカード２２０側に電源監視回路３３０が設けられているが、本体側に設けるようにしてもよい。

【００７８】また、ＰＮＧ情報２１０ｐはＩＣカード２２０側に書き込まれたものを用いたが、ＰＮＧ変更フラグとともに番組情報の中に含ませて放送局側から送り、デコーダ側でＩＣカード２２０のマイコンシステムが、番組情報に含まれたＰＮＧ情報２１０をＰＮ発生器３１０に書き込むようにしてもよい。

【００７９】さらに、ＰＮ発生器３１０は、ＰＮ信号生成のためのロジックが変更可能であればよいので、図１および２の構成に限られない。例えば、ＬＦＳＲの段数を等価的にかえるように構成であってもよく、この場合、電気的にプログラム可能なロジック、例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）などを用いて構成することができる。この場合でもＩＣカード２２０のマイコンシステムがＰＮＧ情報２１０をＰＮ発生器３１０に書き込むことによってＰＮ発生器３１０の動作を変更することができる。

【００８０】また、図３において、ロジック回路部はＮＦ２１２ａ～２１２ｃを用いているが通常のロジックＩＣを用いて一定のロジックを構成するようにしてもよい。

【００８１】

【発明の効果】以上の通り、本願請求項１に係る発明によれば、その構成を容易に知り得ないため、機密性を保持することができ、デコーダのセキュリティを高いものにすることができる。

【００８２】本願請求項２，３又は４に係る発明によれば、ＰＮ発生器が、上記の順次状態遷移するレジスタおよび非線形ロジック又はロジック回路部で構成されるこ

とにより、よりその内部構成を外部から分かりにくくできる。

【００８３】本願請求項５に係る発明によれば、ＩＤとが一致したときにスクランブルキーがＰＮ発生器にあたえられることにより、個別の条件に応じてデスクランブルを行いうる。

【００８４】本願請求項６に係る発明によれば、ＩＣカードが本体に挿入されたときに、ＰＮ信号生成ロジックを定めるための情報がＰＮ発生器にあたられることにより、電源オフ時にその内容が消えてしまってもよいような回路でもよいので、ハードウェアのコストが安いものにし得る。

【００８５】本願請求項７に係る発明によれば、起動時にＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえるので、電源オフ時にＰＮ信号生成ロジックを定めるための情報を保持しなくてもよい構成にし得る。

【００８６】本願請求項８に係る発明によれば、ＰＮ信号生成ロジックの変更を示すＰＮＧ変更フラグがスクランブルされた信号とともに送られたときにＰＮ信号生成ロジックを定めるための情報をＰＮ発生器にあたえるので、ＰＮ発生器の動作は番組に応じて変えることができるため、番組についても機密性を保持することができ、番組のセキュリティも高いものになる。

【００８７】本願請求項９に係る発明によれば、ＰＮＧ選択情報とＰＮＧ変更フラグとが送られたときに、ＰＮＧ選択情報に応じたＰＮ信号生成ロジックを定めるための情報を選択してＰＮ発生器にあたえるので、ＰＮ信号生成ロジックの選択の幅が広くなると共にＰＮ発生器の動作は番組に応じて変えることができるため、番組についてもより機密性を保持することができ、番組のセキュリティもより高いものになる。

【００８８】本願請求項１０に係る発明によれば、ＩＤメモリに記憶されたＩＤとＩＣカード上のＩＤとが一致したときにのみスクランブルキーをＰＮ発生器にあたえることにより、機器のセキュリティをより高めることができる。

【００８９】本願請求項１１に係る発明によれば、ＩＤメモリに記憶されたＩＤとＩＣカード上のＩＤとが一致したときにのみスクランブルキーがＰＮ発生器にあたえられ、ＩＤが一致したときにのみデコーダ本体の使用が可能になるので、デコーダ本体のセキュリティがより高いものになる。

【図面の簡単な説明】

【図１】第１の実施例にかかるデコーダの構成を示した図。

【図２】ＰＮ信号生成のためのロジックが変更可能なＰＮ発生器の構成例を示した図。

【図３】ＰＮ信号生成のためのロジックが変更可能なＰＮ発生器の構成例を示した図。

【図４】第２の実施例にかかるデコーダの構成を示した図。

【図５】第３の実施例にかかるデコーダの構成を示した図。

【図６】第４の実施例にかかるデコーダの構成を示した図。

【図７】第５の実施例にかかるデコーダの構成を示した図。

【図８】第６の実施例にかかるデコーダの構成を示した図。

【図９】スクランブル放送システムの構成図。

【図１０】従来例にかかるデコーダの構成を示した図。

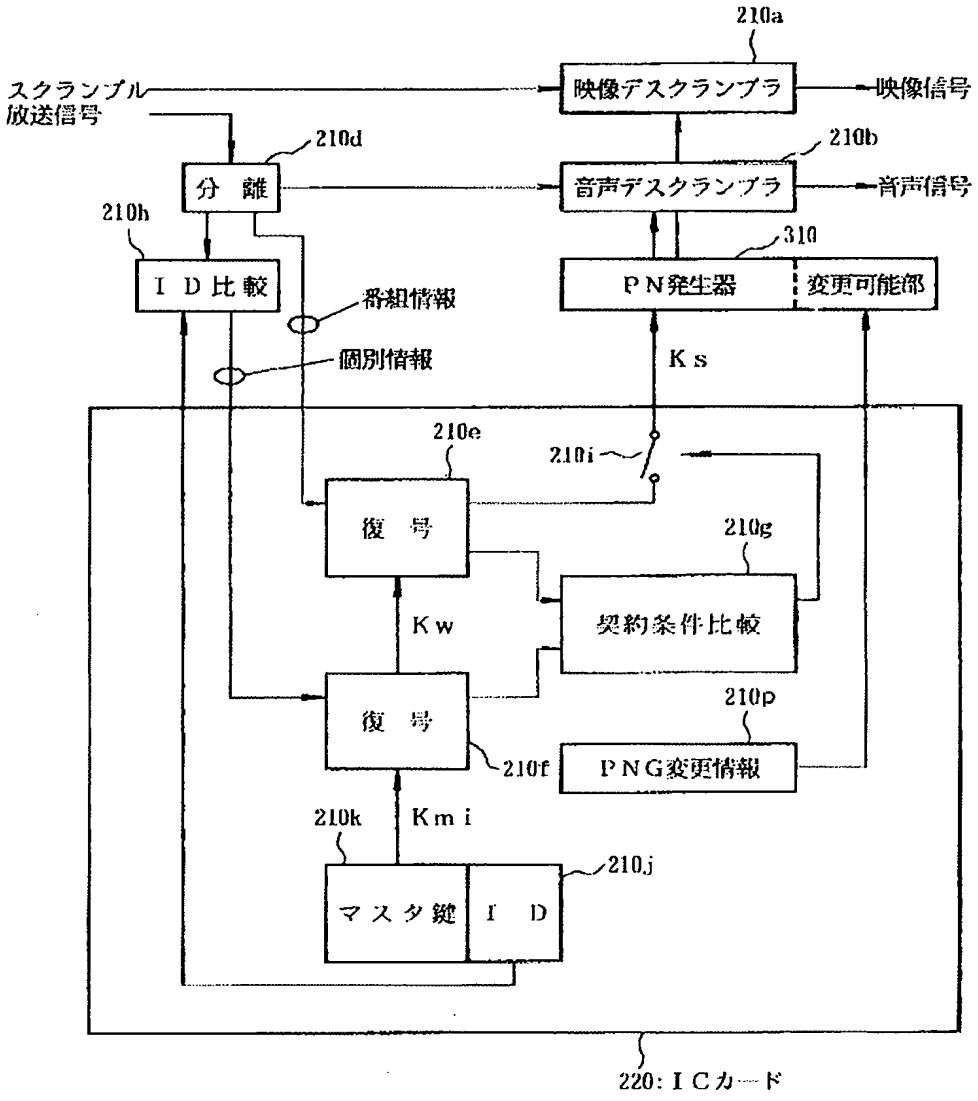
【図１１】従来例にかかるＰＮ発生器の構成例を示した図。

【図１２】ＬＦＳＲの構成例を示した図。

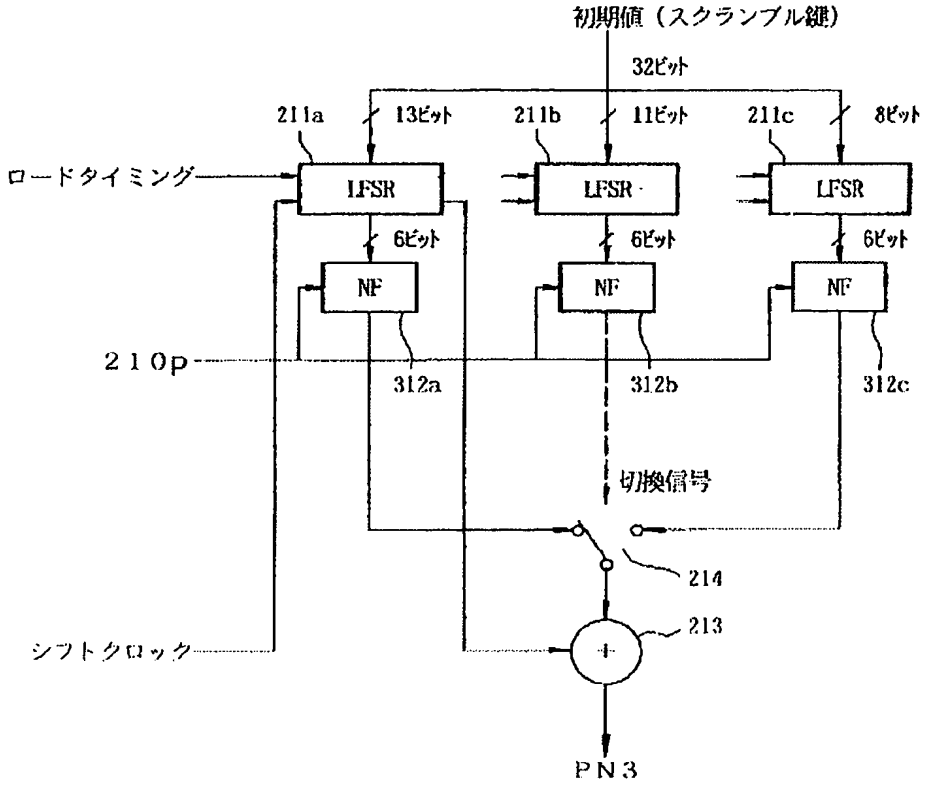
【符号の説明】

２１０ａ…映像デスクランブラ，２１０ｂ…音声デスクランブラ，２１０ｊ…ＩＤ，２１０ｐ，２１０ｐ１，２１０ｐ２…ＰＮＧ情報，２１１ａ～２１１ｃ…ＬＦＳＲ，２２０…ＩＣカード，３１０…ＰＮ発生器，３１２ａ～３１２ｃ…ＮＦ，３１５ａ～３１５ｃ…マルチプレクサ，３３０…電源監視回路，３４０…ＩＤメモリ，４１０ｈ…ＩＤ比較器。

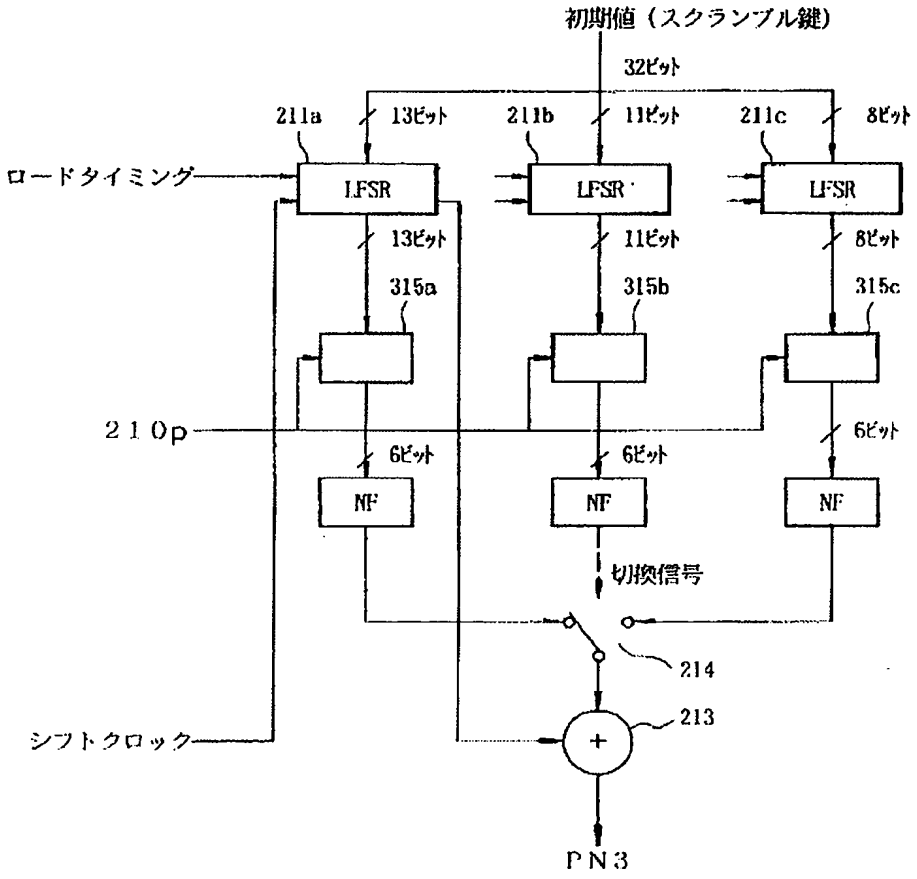
【図１】


210a
スクランブル
放送信号
映像デスクランブラ
映像信号
210d
分　離
210b
音声デスクランブラ
音声信号
210h
ＩＤ比較
310
ＰＮ発生器
変更可能部
番組情報
個別情報
Ｋｓ
210e
210i
復　号
210g
Ｋｗ
契約条件比較
復　号
210p
210f
ＰＮＧ変更情報
210k
Ｋｍｉ
210j
マスタ鍵
ＩＤ
220：ＩＣカード

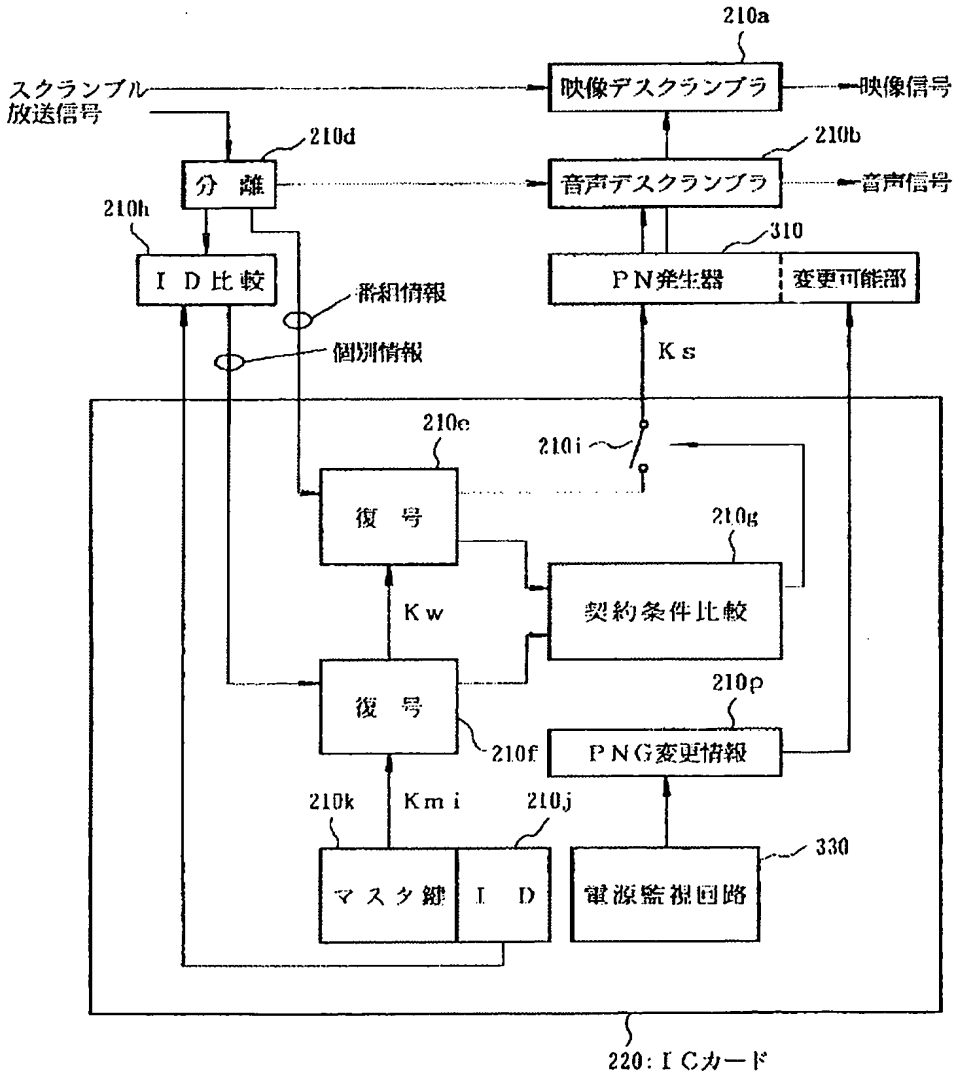
【図２】


初期値（スクランブル鍵）
32ビット
211a
13ビット
211b
11ビット
211c
8ビット
ロードタイミング
LFSR
LFSR
LFSR
6ビット
6ビット
6ビット
NF
NF
NF
210p
312a
312b
312c
切換信号
214
213
シフトクロック
PN3

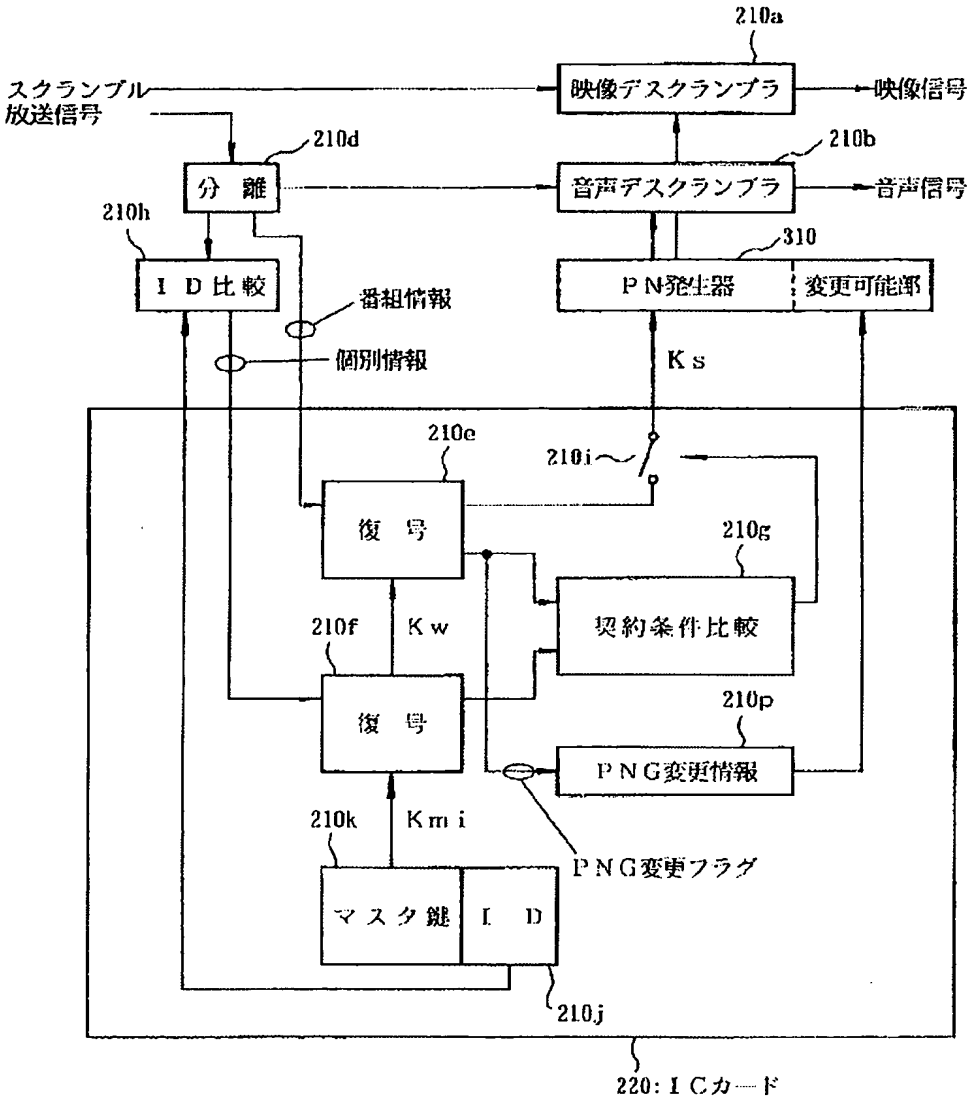
【図３】


初期値（スクランブル鍵）
32ビット
211a
13ビット
211b
11ビット
211c
8ビット
ロードタイミング
LFSR
LFSR
LFSR
13ビット
11ビット
8ビット
315a
315b
315c
210p
6ビット
6ビット
6ビット
NF
NF
NF
切換信号
214
213
シフトクロック
+
PN3

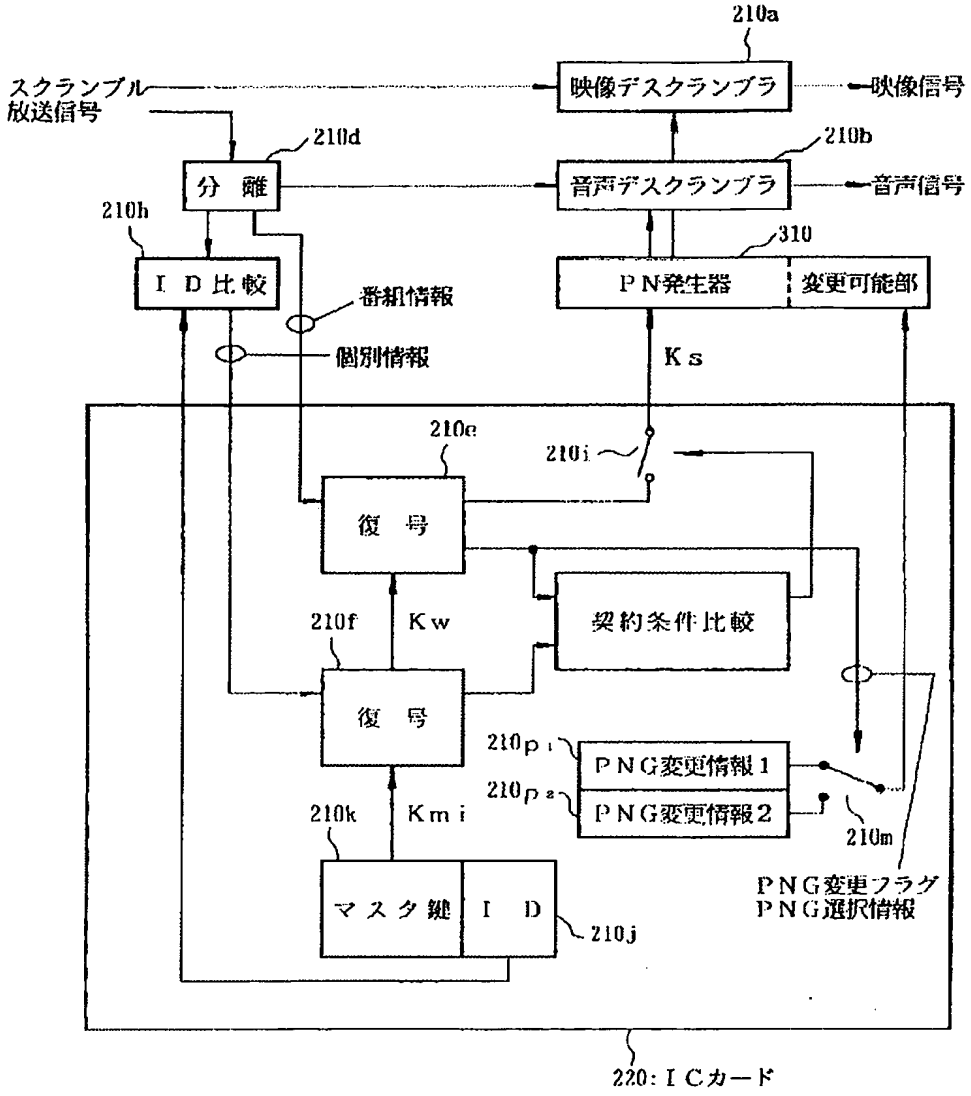
【図４】


210a
スクランブル
放送信号
映像デスクランブラ
映像信号
210d
分　離
210b
音声デスクランブラ
音声信号
210h
ＩＤ比較
番組情報
個別情報
310
ＰＮ発生器
変更可能部
Ｋｓ
210e
210i
復　号
210g
契約条件比較
Ｋｗ
復　号
210p
210f
ＰＮＧ変更情報
210k
Ｋｍｉ
210j
330
マスタ鍵
Ｉ　Ｄ
電源監視回路
220：ＩＣカード

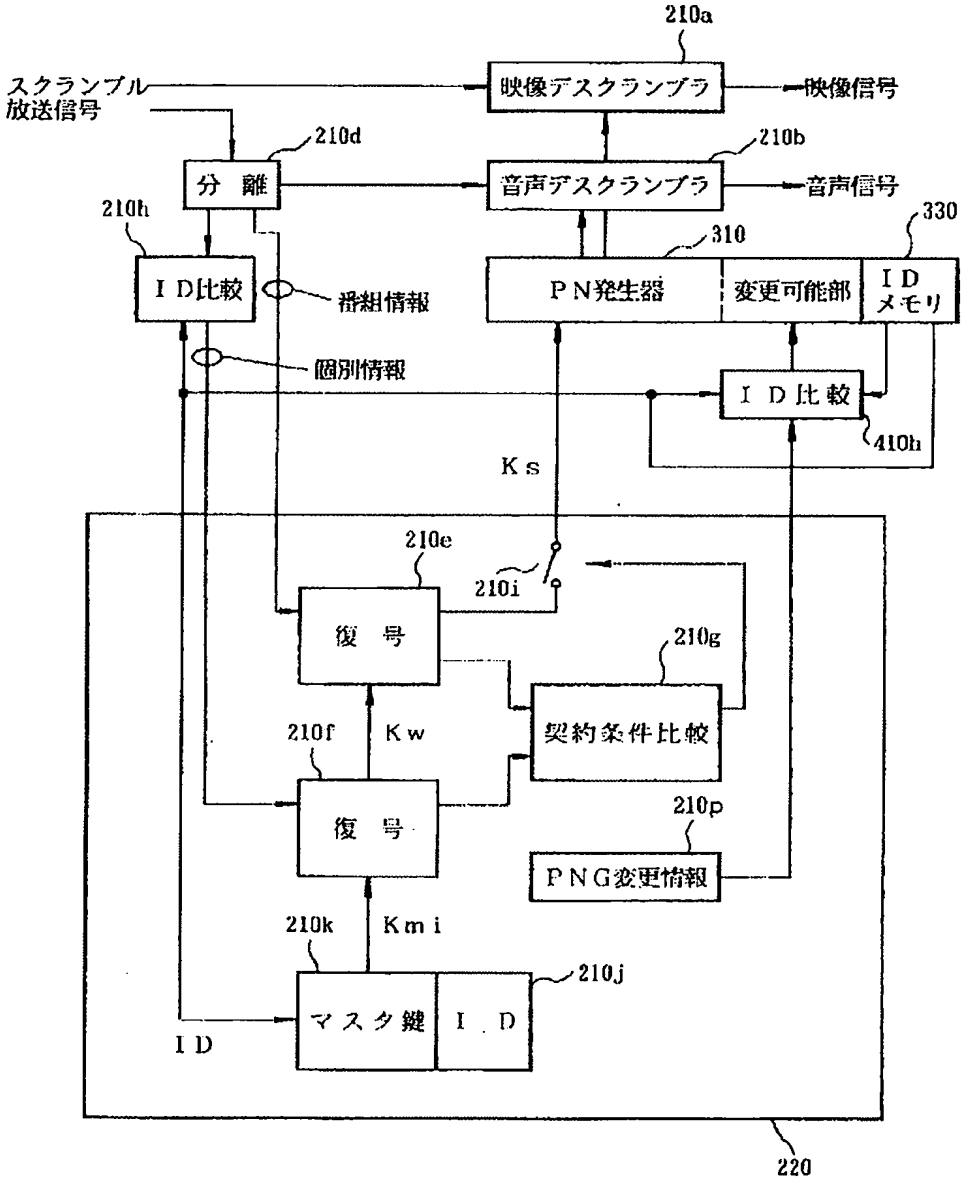
【図５】


210a
スクランブル放送信号
映像デスクランブラ
映像信号
210d
分　離
210b
音声デスクランブラ
音声信号
210h
310
ＩＤ比較
番組情報
ＰＮ発生器
変更可能部
個別情報
Ｋｓ
210e
210i
復　号
210g
契約条件比較
210f
Ｋｗ
復　号
210p
ＰＮＧ変更情報
210k
Ｋｍｉ
ＰＮＧ変更フラグ
マスク鍵
ＩＤ
210j
220：ＩＣカード

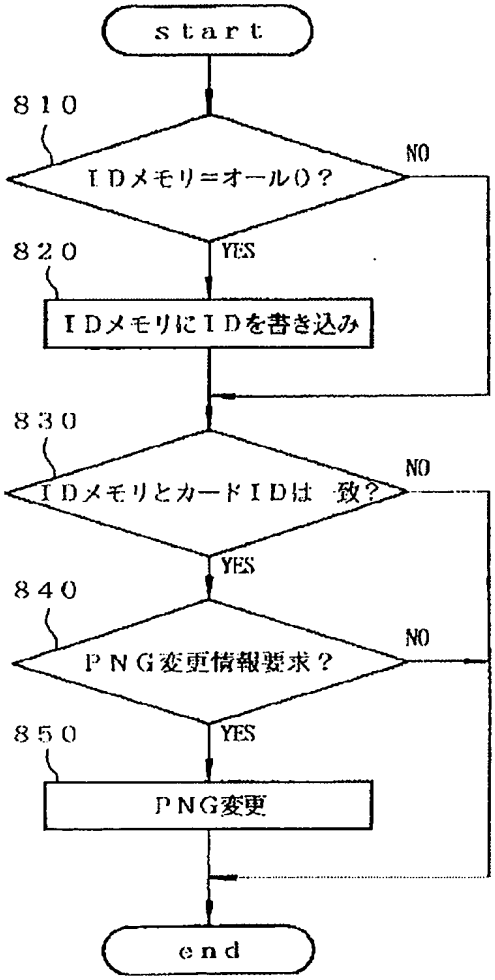
【図６】


210a
スクランブル放送信号
映像デスクランブラ
映像信号
210d
分　離
210b
音声デスクランブラ
音声信号
210h
ＩＤ比較
番組情報
個別情報
310
ＰＮ発生器
変更可能部
Ｋｓ
210e
210i
復　号
契約条件比較
210f
Ｋｗ
復　号
210p1
ＰＮＧ変更情報１
210p2
ＰＮＧ変更情報２
210k
Ｋｍｉ
210m
ＰＮＧ変更フラグ
ＰＮＧ選択情報
マスタ鍵
ＩＤ
210j
220：ＩＣカード

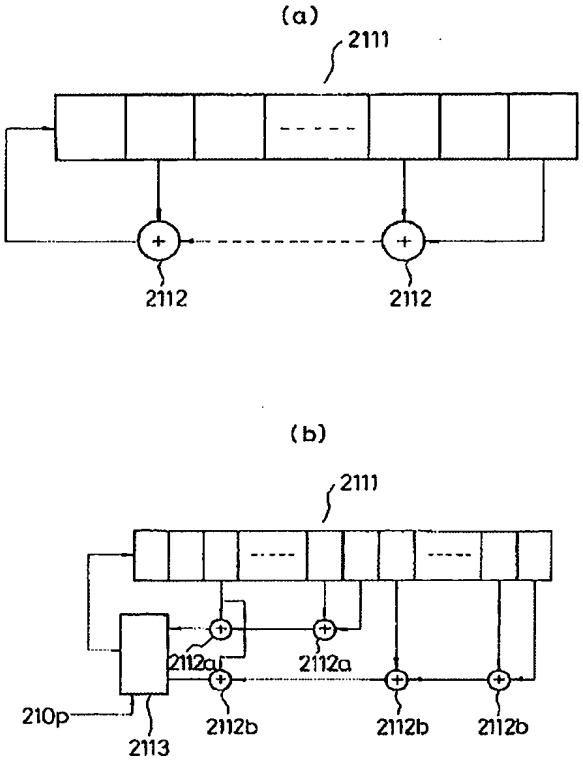
【図７】


210a
スクランブル放送信号
映像デスクランブラ
映像信号
210d
分　離
210b
音声デスクランブラ
音声信号
210h
330
310
ＩＤ比較
番組情報
ＰＮ発生器
変更可能部
ＩＤメモリ
個別情報
ＩＤ比較
410h
Ｋｓ
210e
210i
復　号
210g
契約条件比較
210f
Ｋｗ
復　号
210p
ＰＮＧ変更情報
210k
Ｋｍｉ
210j
マスタ鍵
ＩＤ
ＩＤ
220

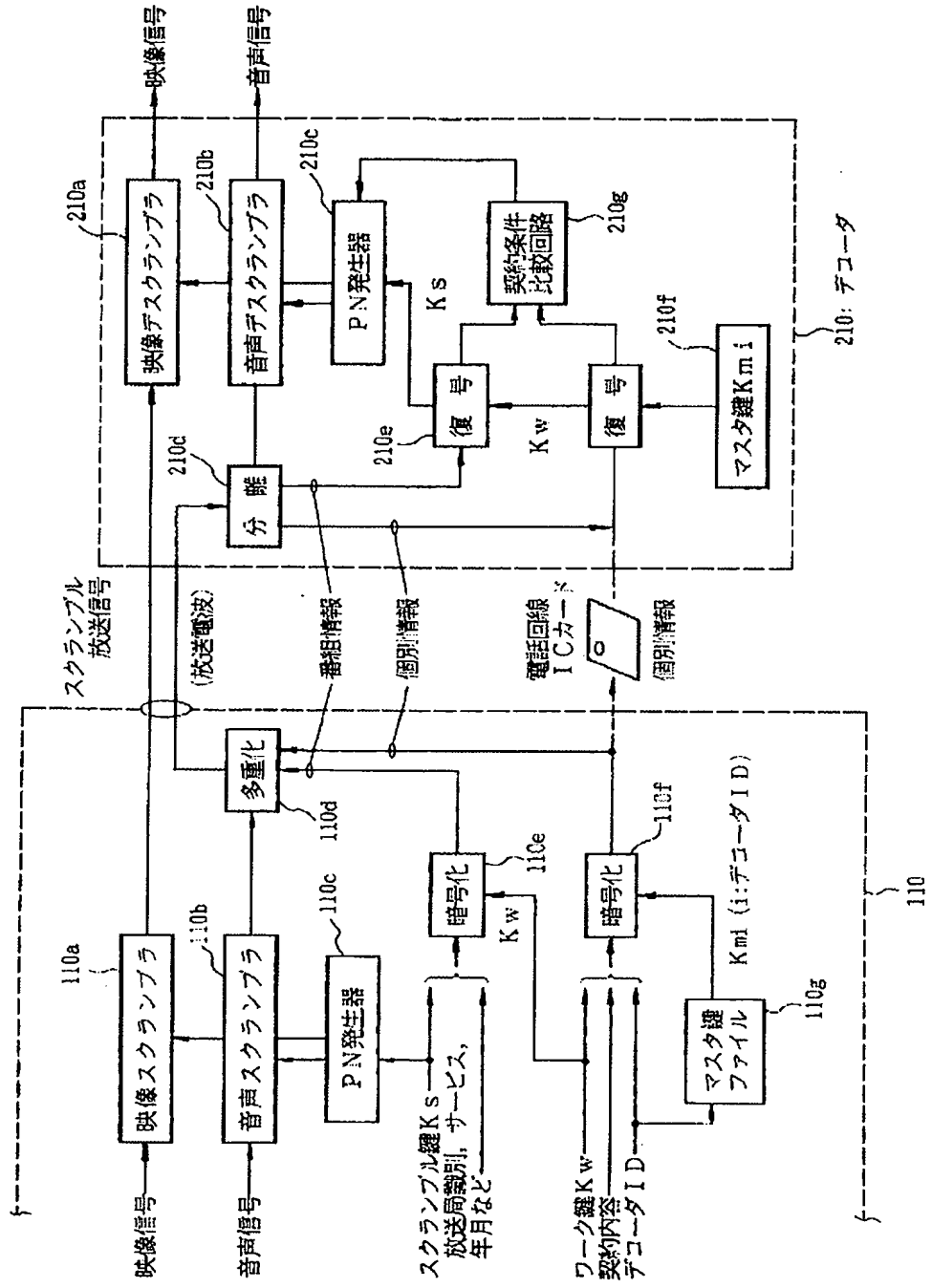
【図８】


start
810
IDメモリ＝オール0？
NO
YES
820
IDメモリにIDを書き込み
830
IDメモリとカードIDは一致？
NO
YES
840
PNG変更情報要求？
NO
YES
850
PNG変更
end

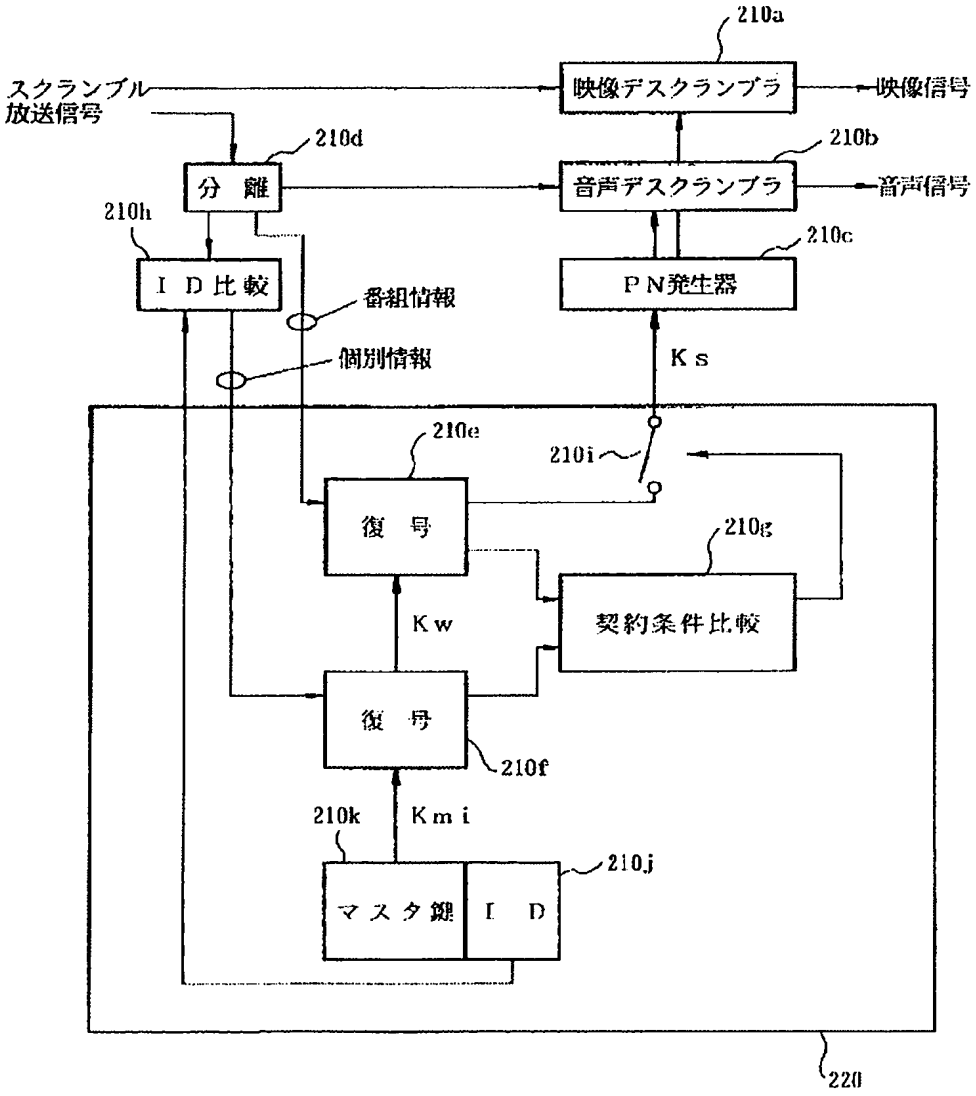
【図１２】


(a)
2111
2112
2112
(b)
2111
2112a
2112a
2112b
2112b
2112b
210p
2113

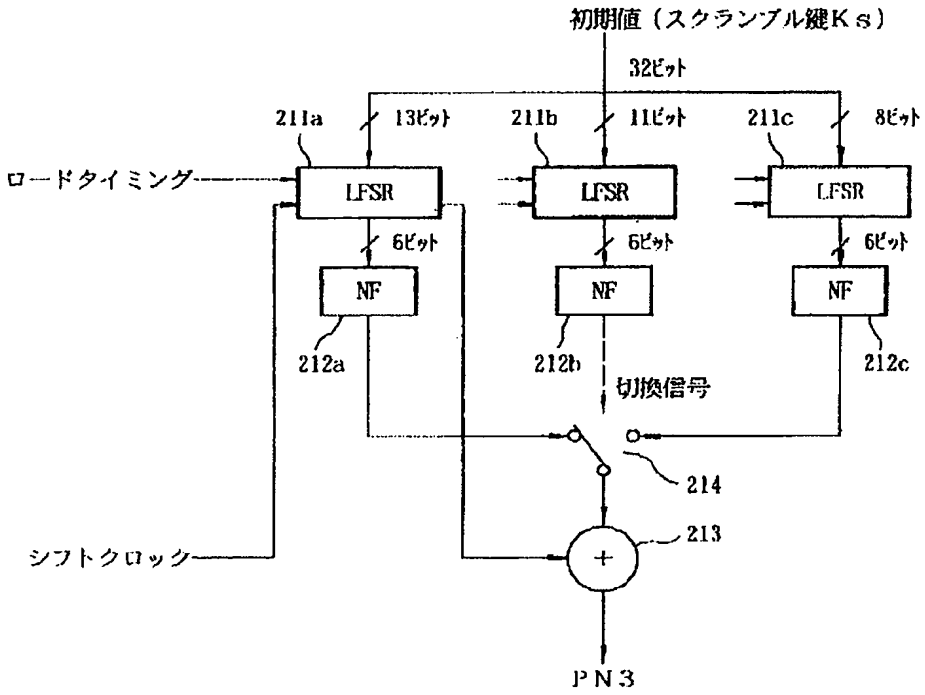
【図９】


映像信号
音声信号
210a
映像デスクランブラ
210b
音声デスクランブラ
210c
PN発生器
Ks
契約条件比較回路
210g
210d
分離
210e
復号
Kw
復号
210f
マスタ鍵Kmi
210: デコーダ
スクランブル放送信号
(放送電波)
番組情報
個別情報
電話回線
ICカード
個別情報
多重化
110d
暗号化
110e
暗号化
110f
110a
映像スクランブラ
110b
音声スクランブラ
110c
PN発生器
マスタ鍵ファイル
110g
Kmi (i:デコーダID)
110
映像信号
音声信号
スクランブル鍵Ks
放送局識別，サービス，年月など
ワーク鍵Kw
契約内容
デコーダID

【図１０】


210a
スクランブル
放送信号
映像デスクランブラ
映像信号
210d
分　離
210b
音声デスクランブラ
音声信号
210h
ＩＤ比較
番組情報
210c
ＰＮ発生器
個別情報
Ｋｓ
210e
210i
復　号
210g
Ｋｗ
契約条件比較
復　号
210f
210k
Ｋｍｉ
マスタ鍵
ＩＤ
210j
220

【図１１】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ 9/28				